엔터프라이즈 네트워크에서 인터넷 웜의 탐지 방법

2006

조용권

석사 학위 논문

엔터프라이즈 네트워크에서 인터넷 웜의 탐지방법

조 룡 권 (赵 龙 权)

정보통신학과 (네트워크 전공)

포항공과대학교 정보통신대학원

2006

엔터프라이즈 네트워크에서
인터넷 웜의 실시간 탐지방법

A Real-Time Detection Method for

Internet Worms on Enterprise Networks

A Real-Time Detection Method for Internet Worms

on Enterprise Networks

by

LONGQUAN-ZHAO

Department of Computer and Communications Engineering

POSTECH Graduate School for Information Technology

A thesis submitted to the faculty of POSTECH Graduate School for Information Technology in partial fulfillment of the requirements for the degree of Master of Engineering in the Department of Computer and Communications Engineering.

Pohang, Korea

December 21, 2005

Approved by

_____

Major Advisor: James Won-Ki Hong

엔터프라이즈 네트워크에서 인터넷 웜의 탐지방법

조 룡 권

위 논문은 포항공과대학교 정보통신대학원 석사 학위논문으로 학위논문 심사위원회를 통과하였음을 인정합니다.

2005년 12월 21일

학위논문심사 위원회 위원장 홍원기 (인)

위 원 서영주 (인)

위 원 송황준 (인)

MCC
20042622

조 룡권 , LONGQUAN ZHAO, A Real-Time Detection Method for Internet Worms on Enterprise Networks , 엔터프라이즈 네트워크에서 인터넷 웜의 실시간 탐지방법, Department of Computer and Communications and Engineering, 2006, 40P, Advisor: J.Won-Ki Hong, Text in Korean

ABSTRACT

The enterprise networks are suffering from the battle with the Internet worm. After the slammer worm's outbreak in 2003, the subject of detection Internet worm became the most important issue on the area of network security. One of most popular systems to detect internet worms are signature based IDS (intrusion detection system) on local networks. Signature based (misuse) IDS defines sets of rules with signatures and detect worms by matching the packets to the rules. This kind of IDS systems need to compare the whole packet include packet payload to the rule set so require long processing time. Another problem of signature based IDS system is that it can not detect new kind of worms because it does not have signatures of new worms. Global scope detection algorithms are the other most popular solution to detect internet worms. These kinds of algorithms are not easy to implement on local networks and are not suitable to the enterprise networks. Real-time requirement is an important factor for a worm detection system. Many real-time solutions are focused on the meaning of detecting worms in the early stage of its breakout. They seldom

mention about the other meaning of real-time, to minimize the processing time. In this thesis, we propose an Internet worm detection method, which is easy to implement on local networks. The proposed algorithm is traffic behavior based detection and thus can detect internet worms in real-time. To validate our algorithm, we first developed Worm Traffic Generator which could generate the scanning traffic of the Internet worms. The Generator has a very user-friendly UI so that the users could generate the worm traffic by simply clicking buttons or inputting values. We utilized this tool to generate quantity worm traces. The real time detection system which implemented by the proposed algorithm detected all kind of these worm traces. We also deployed the detection system on our campus network and analyzed the detection results.

목 차

그림 목차

표 목차

1 서론

인터넷이 발달하고 이를 사용하는 사용자 수는 계속적으로 증가하면서 많은 네트워크 서비스 또한 만들어지고 있다. 이러한 인터넷의 성장과 더불어 다양한 네트워크 보안 공격에 대한 위협들도 증가하였다. 1988년 Morris[1] 웜의 출현 이래로 인터넷 웜에 의한 보안 공격들은 계속 증가되어 왔고, 날로 그 피해가 심화 되여 가고 있다. 35만9천여 호스트를 감염시킨 CodeRed[2]와 10분만에 7만5천여 호스트를 감염시킨 Slammer[3]웜이 그 대표적 예로써 그 손실은 수백만, 수천만 달러에 달한다. 또 인터넷 웜은 그 전파 방법과 수단이 날로 발전하여 은밀하고 탐지하기가 갈수록 어려워 지고 있다.

인터넷 웜은 “네트워크를 통해 사용자의 개입이 없이 스스로 복사 전파하면서 취약점이 있는 서비스를 공격하는 악성코드”이다 [4].

인터넷 웜은 네트워크를 통하여 전파됨으로 전파 과정에 일정한 트래픽 특성을 갖고 있다. 인터넷 웜의 트래픽 특성에 대한 관찰은 인터넷 웜을 탐지하는데 기초적 근거를 제시하여 준다. 사용하는 프로토클, 취약점이 있는 서비스 검색을 위한 스캐닝, 스캐닝을 위하여 타겟을 선정하는 방법 등은 인터넷 웜의 트래픽 특성이다.

인터넷 웜은 전파과정에 TCP 나 UDP 프로토클을 사용한다. CodeRed, Nimda[6], Sasser[7] 그리고 Blaster[5] 등의 대부분의 인터넷 웜들은 TCP 프로토클을 사용하였다. TCP 프로토클을

사용하는 인터넷 웜은 먼저 취약점이 있는 호스트를 검색하기 위하여 타겟을 선정하여 SYN패킷을 보내는데 이 과정은 스캐닝이다. TCP 프로토클을 사용하는 인터넷 웜의 대부분의 트래픽은 이 과정에 발생하게 된다. TCP웜은 가능하면 많은 호스트에 스캐닝을 하여 타겟을 찾아야 함으로 많은 양의 트래픽을 유발하게 된다. TCP와 달리 UDP를 사용하는 인터넷 웜은 SYN 패킷을 보내서 연결을 맺는 과정이 필요 없기 때문에 네트워크 대역폭을 최대한 이용하여 동시에 대량의 웜 본체를 실은 스캐닝 패킷을 전송하게 된다. 대표적인 UDP 인터넷 웜은 Slammer 웜과 Witty[8] 웜이다. 두 인터넷 웜 모두 최대한 이용할 수 있는 대역폭을 사용하여 스캐닝동시에 웜 본체를 발송하여 웜 본체의 크기가 작고 트래픽 양이 크다는 특징들을 갖고 있다.

인터넷 웜은 취약점이 존재하는 서비스나 호스트 혹은 네트워크를 타겟으로 감염을 시도한다. 즉 취약점이 존재하는 포트를 목표로 하기 때문에 인터넷 웜이 발생시에 많은 패킷이 특정포트에 몰리는 트래픽 현상을 보인다. 하나의 인터넷 웜이 여러 가지 취약점을 이용하여 탐지와 제어를 피해가는 것은 Nimda[6]웜이 출현한 이래 많은 인터넷 웜에서 사용하는 방법이 되고 있다.

인터넷 웜은 취약점이 있는 타겟을 스캐닝 할 때, 순차적 방법이거나, 랜덤 방법을 사용하게 된다. 순차적 방법이란, 어떤 초기 타겟의 IP 주소로부터 시작한 순차적인 한 개 블록의 IP주소에 대하여 스캐닝 하는 것이다. 순차적 스캐닝은 타겟 IP주소가 순차적으로 증가하는 트래픽 특성을 보여주고 있다. Blaster는 전체

스캐닝의 60%의 경우 감염한 대상 호스트로부터 시작한 20개의 순차적 IP주소를 스캐닝 하였다[9]. 다른 하나의 가장 대표적인 스캐닝 방법은 랜덤 스캐닝으로 타켓 으로 할 IP 범위를 결정하고 선정된 IP 범위 내에서 랜덤으로 스캐닝을 실행한다. SQL Slammer나 CodeRed 같은 대부분의 웜은 IPv4 전체 대역을 범위로 하고 랜덤 스캐닝을 하였다. 이런 랜덤 스캐닝은 존재하지 않는 IP주소나 존재하지 않는 호스트, 존재하지 않는 서비스로 패킷을 보내는 특성을 갖고 있다. 랜덤 스캐닝은 타겟 IP 범위를 조절할 수 있는데 ARP Routing Table에 근거하여 Routing 가능한 Network 대역, IANA IP v4 Allocation Table[10] 혹은 Bogon List[11]를 참조하여 존재하는 범위의 IP 대역 등을 그 범위로 선정하여 스캐닝 하는 방법도 존재하지만[12] 아직까지는 이런 스캐닝의 기술을 사용한 인터넷 웜이 출현되지 않고 있다. 그 원인은 이런 세밀한 방법으로 IP범위를 선정하여 스캐닝 하려면, 그런 리스트를 인터넷 웜 본체에 실어야 하고 그것은 결국 인터넷 웜의 크기를 늘리게 되며, 나아가서는 전파속도를 현저히 저하시키기 때문이다.

인터넷 웜의 탐지에 관한 연구는 인터넷 웜의 발생한 시작부터 지속적으로 진행 되여 왔으며 특히 2003년 Slammer웜의 출현된 이래, 네트워크 보안 분야에서 가장 중요한 이슈의 하나로 떠올랐다. 대부분의 연구활동은 인터넷 전체 대역에 대한 분산된 모니터링 기법으로 인터넷 웜을 조기에 탐지하는 방법을 제시하고 있다. [13,14,15,16] 이런 방법의 문제점은 모니터링 하는 네트워크의 범위가 커서 국가간, ISP간 혹은 대형회사 간의 상호협력과 연동이

필요하다는 것이다. 이런 방법은 로컬이나 Enterprise네트워크에 적합하지 않으며 또 적용할 수도 없다[17].

많은 로컬이나 Enterprise 네트워크의 관리자들은 IDS 시스템을 도입하여 인터넷 웜을 탐지하는데 적용한다. 이런 IDS 시스템은 수집한 패킷의 전체를 signature와 비교해야 하여 많은 처리시간을 요하게 되며 또한 새로운 인터넷 웜의 signature를 가지고 있지 않아 새로운 웜에 대응할 수 없다.

로컬이나 Enterprise 네트워크에 적응하는 알고리즘을 제안한 연구로는 Qin 등의 연구[18]가 있다. 이 연구에서는 인터넷 웜이 존재하지 않는 로컬 네트워크에서 새롭게 나타나는 웜에 대한 탐지에 초점을 두고 있다.

본 논문은 엔터프라이즈 네트워크에서 실시간으로 인터넷 웜 행위를 탐지하는 방법을 연구하는데 초점을 맞춘다. 대규모 네트워크가 아닌 엔터프라이즈 네트워크를 모니터링의 대상으로 분석하였고, 오프라인이 아닌 실시간 탐지를 목표로 했으며, Payload를 포함한 signature비교가 아닌 IP header만의 분석을 하였으며, 네트워크에 인터넷 웜이 존재하던 존재하지 않던 내부에서 인터넷 웜에 감염된 호스트를 정확하게 Identify하는데 목적을 두었다. 이런 접근 방법을 통해 간단하면서도 정확한 인터넷 웜 탐지 알고리즘을 설계하였다.

알고리즘의 검증을 위하여 우리는 인터넷 웜 트래픽 발생 툴을

개발하였으며 이 툴을 사용하여 다양한 웜의 트래픽을 발생하여 웜 탐지 알고리즘의 정확하게 인터넷 웜을 탐지하는 것을 검증하였다. 또한 실제 Campus Network에서 시스템을 구현하고 탐지된 인터넷 웜의 트래픽 분석을 통해 인터넷 웜의 특징을 파악하였고 더불어 제시한 탐지 알고리즘을 검증하였다. 제안한 알고리즘에 의해 구현된 시스템은 인터넷 웜을 정확히 탐지 하였을 뿐만 아니라 인터넷 웜과 비슷한 트래픽 특성을 갖고 있는 정상 트래픽도 정확히 분류한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해서 알아보고 3장에서는 로컬 네트워크에 적합한 알고리즘을 제안하고 그에 맞게 설계한 탐지 시스템의 구조를 설명하며 4장에서는 먼저 인터넷 웜 발생 툴에 대한 설명과 더불어 이 툴을 사용하여 알고리즘의 검증결과를 보여주며 5장에서는 탐지시스템을 실제 Campus Network에 구축하여 실시간으로 수집된 인터넷 웜의 탐지결과를 분석하여 알고리즘을 검증하였으며 마지막으로 6장에서는 결론을 짓고 향후 연구방향을 제시한다.

2 관련 연구

인터넷 웜의 탄생된 이래 인터넷 웜의 탐지에 관한 연구는 활발히 진행되어왔으며 지속적으로 진행 되여 갈 것이다. 이번 장에서는 이런 연구에 관한 분류를 통하여 우리가 제안하는 탐지알고리즘의 목표를 명확히 하였다.

2.1 Signature-based 탐지방법

Intrusion Detection System(IDS)은 Enterprise 네트워크에서 가장 선호하는 인터넷 웜 탐지 시스템이다. IDS는 misuse 탐지방법과 anomaly 탐지방법 두 가지가 있는데 misuse 탐지방법이란 네트워크에서 공격성 패킷의 signature를 Database나 Rule Set에 저장하여 네트워크 트래픽에서 같은 signature를 갖고 있는 패킷들을 비정상으로 판단하는 방법이고, anomaly 탐지방법은 정상적인 트래픽 패턴을 모델링 하여 그런 패턴에 맞지 않는 패킷들은 비정상으로 보는 방법이다. 로컬 네트워크에서 가장 많이 사용하는 방법은 misuse 탐지방법으로 트래픽 에 signature와 매칭하는 부분이 존재하면 그 트래픽을 비정상으로 판단한다. 이런 방법이 인터넷 웜의 탐지에 사용 되였을 때 문제점은 두 가지이다. 먼저 이런 시스템은 새로운 유형의 인터넷 웜에 대한 signature를 갖고 있지 않기 때문에 새로운 웜을 탐지할 수가 없다. 다른 한가지 문제점은 signature set과 전체 패킷(header와 payload모두)을 비교하여야 하기 때문에 많은 Processing Time을 요하게 된다. 이는

실시간 탐지 시스템에 적용하기 어렵다는 문제점을 야기하는 것이다. 이런 signature based 탐지시스템의 대표적인 예는 Snort[27]과 Bro[28]를 들 수 있다.

Signature-based IDS시스템에 관한 최근의 연구를 보게 되면 [19]의 Bharath의 방법이다. 이 시스템은 모니터링 부분과 IDS부분으로 나누어져 있으며 모니터링 부분에서 빈도가 높게 출현되는 signature가 IDS에 존재하지 않으면 새로운 signature로 IDS에 업데이트하여 다음부터 같은 트래픽이 검출될 때 그것을 비정상으로 판단할 수 있다. 일정하게 새로운 웜에 대해서 탐지할 수 있게 방법이 개선 되였지만, 많은 처리시간이 수요되는 문제점은 개선할 수가 없다.

우리가 이 논문에서 제안하는 알고리즘은 traffic behavior based 탐지방법으로 인터넷 웜의 스캐닝 특성에 의해서 IP 패킷의 header정보로만 기가 비트 네트워크에서 실시간으로 인터넷 웜을 탐지할 수 있다.

2.2 실시간 탐지 방법

실시간 탐지란 두 가지 뜻을 내포하고 있다. 첫째는 인터넷 웜이 발생했을 때 짧은 시간 내에 그 인터넷 웜을 탐지할 수 있어야 하는 것이고 두 번째는 엔터프라이즈 네트워크에서 수집되는 트래픽을 즉시즉시 처리하여 짧은 시간 내에 수만, 수십만 개의 패킷을 처리할 수 있어야 한다.

많은 연구들이 실시간 탐지에 대해 다루어지고 있지만[16,18,20], 대부분의 연구는 실시간 탐지의 첫 번째 의미에만 목표를 하고 있다. 탐지하는데 걸리는 처리시간에 대하여 언급한 연구는 거의 찾아보기 힘들다. 컴퓨터 시스템이나 네트워크 장비의 자원은 제한 되여 있으므로 짧은 시간 내에 처리하여 자원의 점유시간을 줄여주어야 한다. 우리는 TCP SYN 패킷이나 UDP 패킷의 Header만 수집하여 분석함으로써 전체 처리시간을 줄여 실시간 탐지를 가능케 하였다.

2.3 인터넷 전역을 대상으로 하는 탐지방법

인터넷 웜을 탐지함에 있어서 가장 많이 이루어진 연구는 인터넷 전역을 대상으로 모니터링 하여 분석 탐지하는 방법이다. 인터넷 전역을 대상으로 탐지하는 시스템은 일반적으로 분산된 여러 기점의 모니터링과 모니터링 데이터를 분석하는 중앙지점의 탐지 분석하는 부분으로 나누어 구성된다. 모니터링 시점에서 수집하는 데이터의 종류와 탐지분석 기법의 다름으로 하여 수학적 모델링방법, ICMP type 3 탐지방법 외 각 로컬네트워크의 비정상 트래픽을 보안업체에서 수집하여 조기에 탐지하는 방법 등 몇 가지로 분류할 수 있다.

2.3.1 수학적 모델링방법

수학적 모델링 기법을 사용하여 인터넷 웜을 탐지하는데 가장 앞서 갔던 연구는 Zou [14]의 Epidemic Model을 적용한 연구이다. 취약점이 존재하는 호스트 수, 이미 감염된 호스트 수, 인터넷 웜 의

전파속도 사이의 관계가 Epidemic Model을 따른다는 것을 관찰하였고 그에 기초하여 전체적인 인터넷을 모니터링 함으로써 인터넷 웜의 조기 탐지가 가능하게 하였다. Chen [22]은 Analytical Active Worm Propagation(AAWP) 모델을 제안함으로써 랜덤 스캐닝 하는 인터넷 웜의 트래픽 인터넷 웜의 Patching Rate, Death Rate 등을 고려한 탐지 방법을 제시하였다. 또 Jiang[12]은 여러 가지 앞으로 발생 가능한 Selective Random 스캐닝, Routable 스캐닝, Divide and Conquer 스캐닝 기법 (Random Scanning의 여러 가지 유형)을 관찰하고 그 상황을 모델링 함으로써 탐지하는 방법을 제안하였다.

2.3.2 ICMP type 3 메시지를 이용한 탐지방법

하나의 흥미로운 연구는 ICMP type 3 메시지(Destination Port or host unreachable)를 수집하여 탐지하는 방법이다[20]. 이 방법은 전체 인터넷 범위에서 분산된 로컬네트워크들을 모니터링하고 각 로컬 네트워크에서 수집된 ICMP type 3 메시지를 분석하여 인터넷 웜을 탐지한다. 인터넷 웜이 랜덤스캐닝을 하기 때문에 존재하지 않는 호스트나 서비스에 패킷을 전송함으로써 ICMP type 3 메시지가 다량 발생하는 특성을 이용한 것이다.

2.3.3 기타 방법

Symantec[23], CAIDA[24] 등 대형 보안업체는 전 세계의 광범한 User와 로컬 네트워크로부터 비정상 로그를 수집하는 시스템을

구축함으로써 인터넷 웜의 조기 탐지와 경고를 목표로 하고 있다.

이런 Global-Scope을 대상으로 하는 탐지방법은 많은 국가나 ISP, 대형 보안업체들의 공동협력이 필요하기 때문에 그 실현에 여러 어려움이 존재하게 된다. 그리고 이런 탐지방법들은 로컬네트워크를 대상으로 하였을 때 탐지하는 Parameter의 변화 같은 것 들이 너무 미세하고 또 동일한 방법이라도 로컬네트워크에서 구현하기가 어렵기 때문에 로컬네트워크에서 인터넷 웜을 탐지하는데 적용될 수 없다.

2.4 Local Network Detection

로컬 네트워크에서 인터넷 웜을 적시적으로 탐지하는 시스템을 구축하는 것은 인터넷 웜의 감염원을 조기에 발견하고 차단할 수 있는 가장 효과적인 방법이다. 로컬 네트워크 단위의 탐지시스템의 구현은 용이하여 정형화된 탐지방법을 보급화한다면 전체적인 네트워크에서의 조기탐지가 가능해질 것이다.

2.4.1 Destination Source Correlation(DSC) 탐지방법

[18]에서 Qin은 로컬네트워크에 적합한 Destination Source Correlation 알고리즘을 제안하였다. 이 방법은 In-Outbound 트래픽을 수집하고 두 가지 트래픽 사이의 연관되는 상호관계에 의해 인터넷 웜을 탐지한다. 이 알고리즘은 감염되지 않은 로컬 네트워크에서 아주 효과적이나 이미 인터넷 웜에 감염된 환경의

네트워크에서는 그 효력을 발생하지 못하게 된다.

2.4.2 Honey-Net을 이용한 탐지방법

존재하지 않는 Host나 서비스를 실제 존재하는 것처럼 가상화하여 Hacker나 인터넷 웜이 해당 서비스나 Host IP로 스캐닝 행위를 할 때 그 트래픽을 수집하여 비정상 트래픽의 특징을 조기에 파악하여 인터넷 웜의 탐지에 사용하는 방법으로 하나의 서비스나 호스트로 실행하는 것은 Honey-Pot 이고, 여러 개의 Honey-Pot으로 구성된 시스템은Honey-Net 시스템이라고 한다 [25, 21]. Honey-Pot 시스템의 가장 어려운 점은 시스템을 구현하기 어렵고 전체 로컬 네트워크의 IP나 서비스에 대한 수시로 업데이트되는 정보를 확보하여야 한다는 것이다.

2.5 본 논문의 기여

우리는 이 논문에서 Global-Scope네트워크가 아닌 로컬네트워크를 대상으로 용이하고 쉬운 알고리즘을 제안한다. 우리의 알고리즘은 패킷의 Payload가 아닌 패킷의 IP header만으로 탐지의 전반 분석을 진행하게 됨으로써 Processing시간을 최소화하였으며 인터넷 웜의 대표적인 스캐닝 특성에 의한 탐지방법임으로 새로운 웜에 대해서도 탐지가 가능하다. 분산된 시스템이 아닌 Internet Junction에서만 트래픽을 수집함으로 시스템을 용이하게 구현할 수 있다. 제안한 알고리즘은 로컬 네트워크상의 IP 배분현황이나 실행 서비스에 대한

정보를 보유할 필요가 없으며 인터넷 웜에 감염되거나 비 감염상태 모두 정확하게 인터넷 웜을 탐지할 수 있다.

Worm Traffic Generator를 통하여 인터넷 웜의 스캐닝 패킷들을 발생하였고 그 트래픽을 Worm Detection System이 제대로 탐지하는 것을 확인하였고, 실제 캠퍼스 네트워크에서 구현하고 인터넷 웜을 탐지하고 수집된 인터넷 웜 트래픽의 분석을 진행함으로써 알고리즘을 검증하였다.

3 인터넷 웜의 탐지 알고리즘과 탐지 시스템

이번 장에서는 인터넷 웜의 알고리즘을 설명하고 그 알고리즘에 근거하여 디자인된 탐지시스템을 보여준다.

3.1 인터넷 웜의 탐지 알고리즘

인터넷 웜의 트래픽 특성에 근거하여 우리는 탐지 알고리즘을 제안하였다. 그 알고리즘에 대해서 말하기 앞서 우리는 먼저 인터넷 웜의 스캐닝 특성에 대해서 더 깊이 살펴 보도록 한다.

인터넷 웜의 가장 큰 악 영향은 과다한 트래픽 양으로 하여 네트워크의 마비를 일으키는데 있다. 이런 과다한 트래픽 양은 인터넷 스캐닝 단계에 대부분 발생한다. 때문에 인터넷 웜의 탐지는 인터넷 웜의 스캐닝 단계에 이루어져야 하며 스캐닝 특성을 기초로 하여 분석 되여야 한다. 우리가 제안하는 알고리즘은 인터넷 웜의 스캐닝 특성의 분류를 기초로 그 특성에 맞는 트래픽을 분석함으로써 인터넷 웜을 탐지하였다. 이용한 인터넷 웜의 스캐닝 특성에 대해서 논하자면, 첫째로 인터넷 웜은 특정된 Destination Port로 많은 양의 스캐닝 패킷을 발생한다는 것이다. 엔터프라이즈 네트워크의 한 개 호스트가 거의 동시에 몇 백, 몇 천 개의 패킷을 내보는 경우는 P2P 트래픽이나 인터넷 웜 트래픽을 제외하고는 다른 Application에서는 찾아볼 수 없다[26]. 이런 스캐닝 특징에 근거하여 우리는 인터넷 웜의 탐지방법을 제안하였고 그 구제적 방법은 아래와 같다.

먼저 모니터링 하는 엔터프라이즈 네트워크의 한 호스트에서 한

특정된 Destination Port로 많은 양의 패킷을 발생하는 트래픽을 Suspicious List로 간주하였다. 다음으로 이용한 인터넷 웜의 스캐닝 특성은 Sequential/Random Scanning이다. Sequential웜(예를 들면 Blaster, Scalper 등)은 목적지 주소가 순차적으로 증가하는 특성을 갖고 있으며, Random Scanning 웜 (대 부분의 웜)은 Assign되지 않은 Destination IP 대역에 스캐닝을 하는 특성을 갖고 있다. 우리의 알고리즘은 앞 에서 찾아낸 Suspicious List에서 이런 특성을 갖고 있는 트래픽을 추출하여 인터넷 웜 트래픽 으로 간주 하였다. 마지막으로 우리가 이용한 인터넷 웜의 스캐닝 특성은 In-Outbound 트래픽의 상호관계이다. Inbound Traffic에서도 상응한 Destination Port로 많이 분산된 Destination IP로 패킷 이 흘러 드는 특성을 이용하여 P2P나 정상 트래픽을 분류하였다. 위와 같은 인터넷 웜의 스캐닝 단계에 서 나타내 는 트래픽 특성을 이용하여 우리는 효과적으로 인터넷 웜을 탐지할 수 잇는 알고리즘을 제안한 것이다. 그림 1은 알고리즘의 Flowchart를 보여주고 있다. 그림에서 Dest_IP는 목적지주소를 말하며 flow는 그림 2의 포맷과 같은 3-tuple Packet들의 모음이다.

Flowchart에서 볼 수 있듯이 탐지는 크게 두 개 부분으로 나뉜다. 먼저 Suspicious List를 생성하고 다음에 Suspicious List에서 인터넷 웜 트래픽을 분류해내는 것이다. Suspicious List는 Outbound Traffic의 flow 들로 구성되는데 여기서 말하는 Flow는 일정한 시간 내에 수집된 Destination Port, Protocol, Source Host IP Address가 같은 패킷들의 집합을 말한다[그림 2].

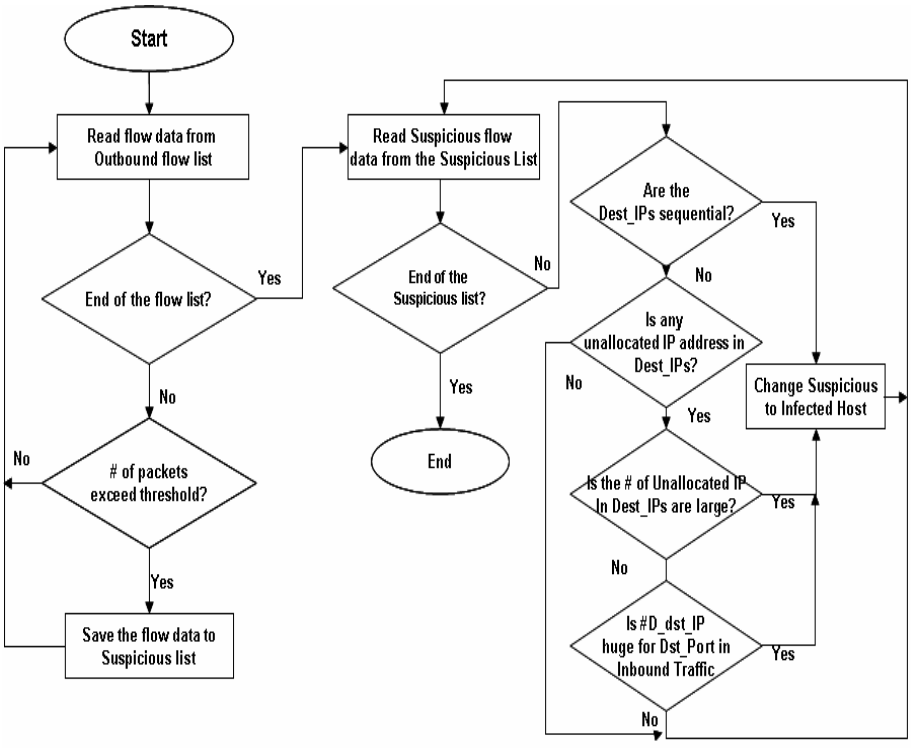

그림 1 The FlowChart of Worm Detection Algorithm

한 Flow의 Packet Count가 Threshold Value를 넘으면 이런 Flow를 Suspicious List에 추가하게 된다. P2P와 인터넷 웜 트래픽을 제외한 다른 트래픽은 발생하는 SYN패킷이 일정한 임계 값을 초과하지 않는다는 연구는 [26]에서 진행된바 있다. Threshold값의 조절로 우리는 P2P나 인터넷 웜 트래픽 만으로 구성된 Suspicious List를 구성할 수 있는 것이다. 모든 Flow에 대해서 다 이런 검증이 끝나면 Outbound Traffic에서의 전체적인 Suspicious List를 얻게 된다. Suspicious List가 구축되면 다음 단계에서는 이 Suspicious List에서 어느 flow가 인터넷 웜 트래픽 인지를 여러 절차에 걸쳐

분석한다. 처음 절차는 flow의 Destination IP Address가 Sequential인지를 체크한다. 만약 Sequential이라면 해당 flow는 인터넷 웜 flow로 판정 되고 해당 Source Host는 인터넷 웜에 감염

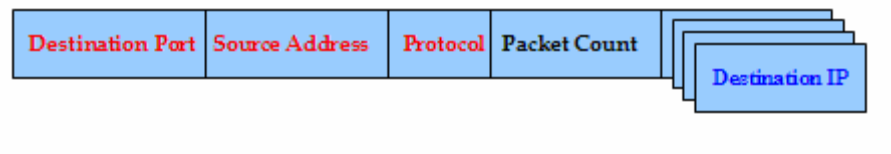

그림 2 The 3-tuple Flow Format

된 것으로 탐지된다. Sequential 하지 않다면 다음 절차는 Destination IP Address 중에 Unallocated IP address 가 있는지를 체크 한다. 여기서 비교하는 대상은 IANA IP v4 Allocation Table[10]로 Destination IP중에 이 Table에서 배정되지 않은 IP를 사용하는 것이 하나라도 존재하는지를 체크한다. 만약 없다면 이런 flow는 정상적인 flow로 보고 다음 flow로 넘어가고 Unallocated IP를 사용한다면 얼마나 많이 사용되는지를 체크한다. Normal Traffic도 간혹 Unallocated IP로 트래픽을 보낼 수 있으므로 일정한 수치이상의 개수가 나오는지를 체크하여 그 이상이면 인터넷 웜으로 판정한다. Unallocated IP 개수가 일정수치 이하로 나오는 flow들은 마지막 비교절차를 거쳐 인터넷 웜인지 아닌지를 판단하게 된다. Inbound Traffic에서 해당 flow의 Destination Port로 Destination IP의 분포도를 관찰하는 것이다. 정상 트래픽은 엔터프라이즈 네트워크의 제한된 IP와 Connection을 맺고 있겠지만, 인터넷 웜 트래픽 같은 경우는 그 취약점이 존재하는 Destination Port로

Distinct Destination IP의 분산도가 높다. Suspicious List에서 Unallocated IP를 사용했던 flow에 존재하는 Destination Port의 Inbound에서의 Distinct Destination IP의 분산도가 높으면 인터넷 웜으로 판단한다. 분산도가 낮은 나머지 flow들은 정상 트래픽으로 분류한다. Figure 2는 알고리즘의 Pseudo Code이다. 알고리즘의 검증은 Worm Traffic Generator를 통한 비교분석(제4장), POSTECH 네트워크에서의 구현(제5장)을 통하여 진행하였다.

```
Pseudo Code of Algorithm
Start
1) 엔터프라이즈 네트워크의 트래픽의 수집
2) 모든 Outbound Traffic에 대한 스캐닝 행위 flow 수집, Inbound Traffic의 Destination Port
   별 Distinct Destination IP의 개수 리스트 생성
3) 스캐닝 행위 flow에서 Packet 수가 임계 값을 넘은 flow로 Suspicious List생성
4) foreach ( flow in Suspicious List) do
5) if(목적지 주소가 순차적이면)
6)          then '인터넷 웜 트래픽으로 판정'
7) else if(목적지 주소에 할당되지 않은 주소가 포함)
8)          then if(할당되지 않은 주소가 임계치 값 이상일 경우)
9)                    then '인터넷 웜 트래픽으로 판정'
10)                   else if(관련 포트의 Inbound Traffic의 Distinct Destination IP 개수가
                                  임계치 값 이상)
11)                             then '인터넷 웜 트래픽으로 판정'
12)                   else '정상 트래픽'
13)         else '정상 트래픽'
14) end
End
```

그림 3 알고리즘의 Pseudo Code

3.2 인터넷 웜 탐지 시스템의 구조

알고리즘에 의하여 구현하는 웜 탐지시스템의 구조는 과 같이 여러 개의 모듈과 Component로 구성 되였다.

3.2.1 패킷의 수집

패킷의 수집은 엔터프라이즈 네트워크가 외부 인터넷과 연결되는 링크에서 이루어진다. 네트워크 링크에 Tap을 물려 수집 하거나 라우터에서 미러링시키는 방법을 사용할 수 있다. 수집되는 패킷은 Payload를 제외한 IP Header만 수집함으로써 처리시간과 처리량을 줄인다. 양방향의 트래픽을 모두 수집하여 스캐닝 성질을 갖는 패킷들 (TCP SYN, UDP packets)만 Flow Generator로 보낸다.

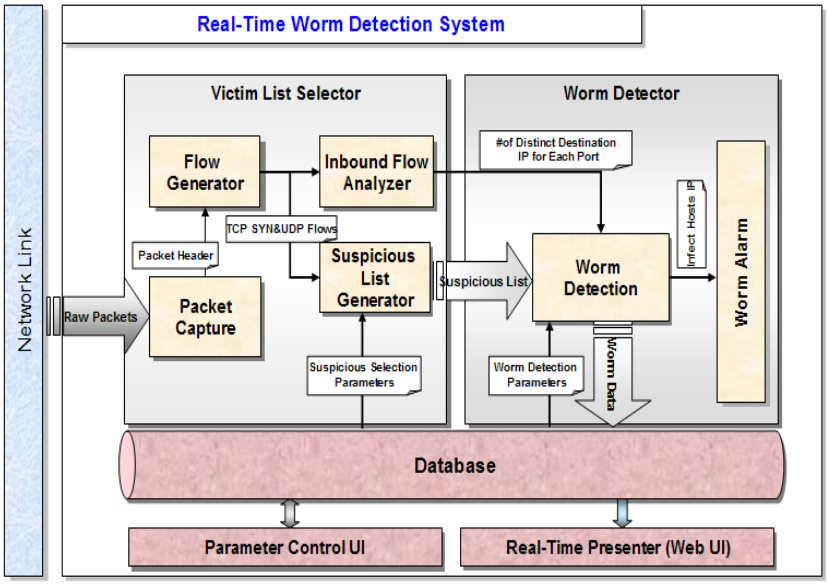

그림 4 탐지시스템의 구조

3.2.2 Flow Generator

Flow Generator에서는 Packet Capture에서 수집된 Scanning Packet을 일정한 Interval Time단위로 3-tuple flow를 구성한다. 3-tuple flow란 Source IP Address, Destination Port, Protocol 세 가지 속성이 같은 Interval time사이에 수집된 패킷들의 집합 정보이다. 이런 세가지 속성이 같은 packet들의 packet count, start time, end time, Destination Host 등의 정보가 flow data에 저장되게 된다. 이런 Flow는 메모리 혹은 HDD에 저장된다. (실시간 탐지를 위해서는 Memory에 저장 되여야 한다.)

3.2.3 Suspicious List Generator

이 모듈은 Network Administrator가 설정한 Threshold 값을 읽어서(파일이나, 데이터베이스) Packet Count가 threshold 값보다 큰 flow들을 suspicious list에 저장한다.

3.2.4 Inbound Flow Analyzer

Inbound Flow Analyzer는 Inbound Traffic에서 각 Destination 포트로의 Destination IP의 분산 도를 측정한다. 모든 port에 대해서 얼마나 많은 서로 다른 목적지 주소로 스캐닝 패킷을 뿌리는지를 Count하여 그 리스트를 메모리에 저장한다.

3.2.5 Internet Worm Detection

Suspicious Flow내의 목적지 주소들의 구성을 관찰함으로써 먼저

그 주소들이 Sequential 하게 분포 되였는지 체크하고 다음에 Unallocated IP주소가 그 중에 존재 하는지를 체크하고 Inbound Flow Analyzer에서 각 포트 별 목적지 주소 분산 도와 비교하여 인터넷 웜의 트래픽을 분류한다. 결과물은 인터넷 웜에 감염된 flow들이다.

3.2.6 Worm Alarm

Internet Worm Detection에서 탐지된 flow내의 Source IP, Destination Port, Time등의 정보로 Administrator에 이 메일이나 실시간 SMS를 보내는 모듈이다. 이 모듈은 Human Intervention으로 인터넷 웜의 전파를 최소화하려는데 그 목적이 있다.

3.2.7 Web UI based Presenter

시스템의 네트워크에 Setup될 때 각 단계에서 사용할 threshold값의 설정 및 조절 등의 Network Administrator의 UI controller와 인터넷 웜 탐지결과를 보여주는 Webpage 생성하는 부분이다. 임계지 값이나 탐지결과는 Database나 File로 저장 되여 탐지시스템의 Main부분과 상호 연동 된다.

3.3 탐지 시스템의 구현

우리는 POSTECH 네트워크에 제안한 구조를 갖는 실시간 탐지시스템을 구현하였다. POSTECH 네트워크는 B 클래스 네트워크로 내부에 6천 여대의 호스트와 서버들로 구성된 엔터프라이즈 성격을 가진

네트워크로서 알고리즘 검증에 적합한 네트워크이다.

3.3.1 POSTECH 네트워크의 구성

그림 5와 같이 POSTECH 네트워크는 두 개의 라우터로 외부 네트워크에 연결 되였고 두 개의 코어 스위치는 두 개의 라우터와 완전

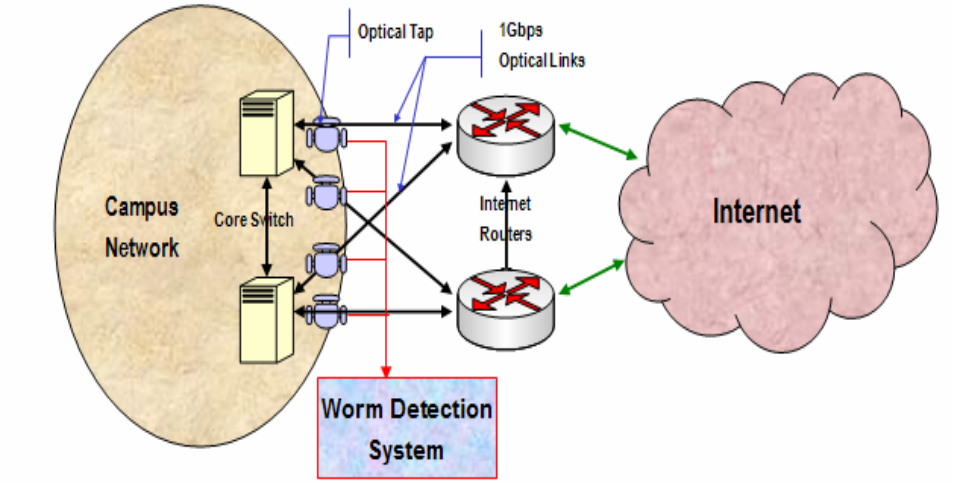

그림 5 POSTECH 네트워크에서 트래픽 수집

연결 방식으로 연결 되여 있다[29]. 이 4개의 연결선에 4개의 Optical tap을 설치함으로써 POSTECH 네트워크에서 흘러가는 전체의 패킷을 수집한다. 수집된 패킷들은 웜 탐지 시스템에 보내서 인터넷 웜 인지를 검사하게 된다.

3.3.2 구현에 사용된 툴과 방법

인터넷 탐지 시스템은 레드헷 리눅스 9.0 OS를 설치한 PC 서버에 구현 되였다. 모든 모듈은 C 언어로 작성 되였고, 사용한 Database는

MySql이다. 결과를 보여주는 웹 페이지는 PHP로 작성 되여 그 결과를 실시간으로 확인할 수 있다.

4 인터넷 웜 탐지 알고리즘의 검증

제안한 알고리즘의 검증을 위하여 우리는 연구실의 스위치 전면에 모니터링 시스템을 구축하였다[그림 6]. 스위치 앞부분에 설치된 리눅스 박스에서 연구실의 내부와 밖으로 흐르는 패킷을 모두 수집하여 제안한 알고리즘에 의해 구현된 Worm Detection System(WDS)에서 탐지결과를 분석하여 알고리즘이 인터넷 웜의 스캐닝 트래픽을 제대로 탐지하는지를 관찰하였다. 이런 검증을 위하여 실험환경을 구축하였고 여러 가지 인터넷 웜의 트래픽을 발생 가능한 Worm Traffic Generator를 개발하였다. Worm Traffic Generator를 이용하여 Global-Random, Global-Sequential, Local-Random, Local-Global 웜의 트래픽을 발생하여 탐지 결과를 분석하였다.

4.1 실험환경

실험에서 사용된 Switch Hub에 연결 되여 있는 Host수는 대략 10대였고 그 중에 한 Host는 Worm Traffic을 Generate하기 위하여 사용 되였다. 다른 Host들은 연구실에서 정상적으로 사용되는 Host였으며 전부 Windows XP를 OS로 사용하고 있다. 모든 내부의 Host는 Linux Box내에 설치된 Bridge를 통하여 외부와 Connection을 한다. WDS 시스템은 제시한 알고리즘에 근거하여 내부에서 인터넷 웜에 감염된 호스트를 Identify한다. Suspicious List를 생성시 그 임계 값은 1분에 TCP SYN 200 패킷, UDP 1000

패킷이다. Input은 같이 Bridge 를 흐르는 모든 패킷이고 Output은 Suspicious List, 그리고 인터넷 웜에 감염된 flow들이다.

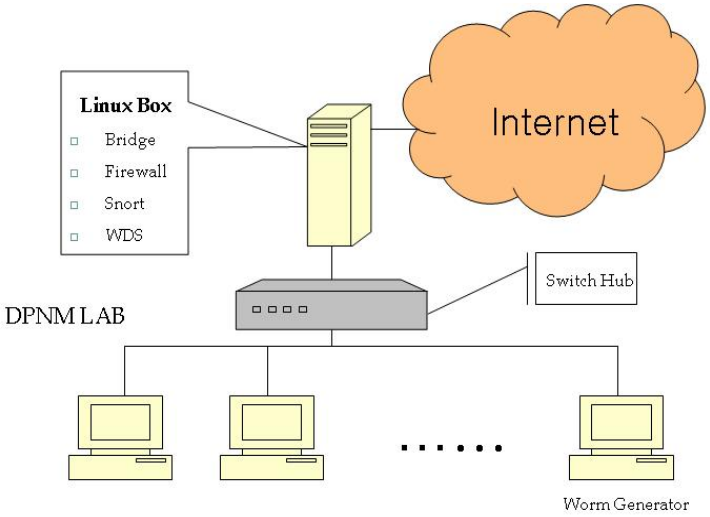

그림 6 알고리즘의 검증을 위한 위한 실험환경

Firewall은 Generate된 인터넷 웜 스캐닝 패킷이 인터넷으로 유출하는 것을 차단해준다. WDS의 False Positive의 측정을 위하여 먼저 실제 인터넷 웜의 코드를 실행시켜 탐지결과를 관찰하였고 다양한 인터넷 웜 트래픽을 생성하기 위하여 자체로 개발한 Worm Traffic Generator를 이용하였다.

4.2 실제 웜코드의 실행을 통한 실험

연구를 위하여 우리는 실제 Decoding 된 인터넷 웜의 C 코드를 확보하였고 이런 실제 코드를 컴파일 실행하여 인터넷 웜의 트래픽을 Generate하였다. 인터넷 웜의 코드는 정확하게 인터넷 웜이 이용했던

포트를 사용하는 것이 아니라 Slammer 웜은 UDP 1178 (1434)포트, Blaster웜은 TCP 128 (135)포트를 사용하였다. 실험은 2005년 09월09일 17시 24분에 Blaster Worm, 23시 48분에 Slammer웜 트래픽을 발생 하였다. WDS의 탐지결과는 각각 [그림 7,그림 8]와 같이 Blaster Worm은 Sequential 로, Slammer웜은 Random Scanning웜으로 판정 하고 있다.

Protocol	Dst_Port	Source Address	Destination Address	Source Port
6	128	141.223.82.168	141.223.67.184	4647
6	128	141.223.82.168	141.223.67.183	4646
6	128	141.223.82.168	141.223.67.182	4645
6	128	141.223.82.168	141.223.67.181	4644
6	128	141.223.82.168	141.223.67.180	4643
6	128	141.223.82.168	141.223.67.179	4642
6	128	141.223.82.168	141.223.67.178	4641
6	128	141.223.82.168	141.223.67.177	4640
6	128	141.223.82.168	141.223.67.176	4639
6	128	141.223.82.168	141.223.67.175	4638
6	128	141.223.82.168	141.223.67.174	4637
6	128	141.223.82.168	141.223.67.173	4636
6	128	141.223.82.168	141.223.67.172	4635
6	128	141.223.82.168	141.223.67.171	4634

그림 7 WDS에서 탐지한 Blaster 트래픽

우리의 알고리즘은 정확하게 실제 웜이 발생한 트래픽을 인터넷 웜으로 판정하였고 내부네트워크의 어떤 호스트가 감염 되였는지를 보여주고 있다. 이런 실제 웜의 코드를 확보하는 데는 일정한 어려움이 있고 다양한 웜 트래픽이 발생시 정상적으로 작동하는지를 검증하여야 할 것이다. 이런 다양한 인터넷 웜의 트래픽의 발생을 위하여 우리는 인터넷 웜의 트래픽 발생 툴 Worm Traffic Generator를 디자인 개발하였고 이를 사용하여 가능한 많은 실험을 할 수 있었다.

Protocol	Destination Port	Source Address	Destination Address	Source Port
17	1178	141.223.82.168	140.192.166.101	2663
17	1178	141.223.82.168	24.236.10.229	2663
17	1178	141.223.82.168	82.143.18.21	2663
17	1178	141.223.82.168	148.219.103.137	2663
17	1178	141.223.82.168	126.207.120.129	2663
17	1178	141.223.82.168	48.150.103.196	2663
17	1178	141.223.82.168	74.161.45.66	2663
17	1178	141.223.82.168	236.74.61.122	2663
17	1178	141.223.82.168	182.159.46.197	2663
17	1178	141.223.82.168	126.241.38.232	2663
17	1178	141.223.82.168	48.224.186.246	2663
17	1178	141.223.82.168	74.51.255.166	2663
17	1178	141.223.82.168	88.76.20.109	2663
17	1178	141.223.82.168	188.129.87.57	2663

그림 8 WDS에서 탐지된 Slammer Worm 웜

4.3 Worm Traffic Generator

그림 9 Worm Traffic Generator의 모듈

여러 가지 인터넷 웜의 스캐닝 트래픽을 Generate하기 위하여 우리는 Worm Traffic Generator를 개발하였다. 우리가 고려한 Worm Traffic Generator의 요구 사항은 다음과 같다.

1) User Friendly Interface: User가 조작하기 쉽고 편리해야 한다.

2) Flexibility: 인터넷 웜의 트래픽 특성 패러 미터로 모든 웜의

스캐닝 패킷을 Generate할 수 있어야 한다.

3) Scalability: Unix 시스템이나 윈도우 시스템에 다 실행가능 해야 한다.

앞에서와 같은 요구 사항으로 디자인된 Generator의 구조는 그림4와 같다. GUI를 통하여 유저는 인터넷 웜의 패러미터를 선택하고 Parameter Aggregation을 통하여 원하는 인터넷 웜을 생성하고 Traffic Generation을 통하여 IP layer 패킷을 생성하여 Thread를 이용하여 트래픽을 생성한다. 인터넷 웜의 트래픽 특성에서 필요한 패러미터는 모두 선택 가능 하기 때문에 여러 가지 인터넷 웜 트래픽을 생성할 수 있다. 예를 들면, TCP 445 포트의 취약점을 이용하는 랜덤 스캐닝 웜의 트래픽을 20초 간격으로 한번에 300패킷씩 발생하고 싶다면 protocol에서 TCP를 선택하고 Destination Port에 445를 입력하고 Interval 값을 20으로 입력하고 Scanning Rate를 300으로 입력하고 Scanning Policy를 Random으로 선택하여 Generate시키면 된다. Protocol, Destination Port, Interval, Scanning Rate, Scanning Policy 등은 모두 이 툴에서 선택 가능한 패러미터인 것이다. 그 외에도 Scanning Range, Worm Body Size, Worm Payload, Number of Infected Host등의 패러미터도 고려하여 조작하기 쉽고 편리한 Worm Traffic Generator를 구현하였다. 우리는 구현된 Generator를 이용하여 Global-Random, Global-Sequential웜, Local-Random, Local-Sequential 웜 트래픽이 발생할 때 Worm Detection System의 탐지결과를 고찰하였다.

4.4 Global-Random 웜의 탐지

2005년 12월 17일 12:37분에 Worm Traffic Generator를 이용하여 Global Random Scanning 웜의 스캐닝 트래픽을 발생하여 그 결과를 관찰하였다. 표 1과 같이 UDP 1434-Random-Unlimited speed 웜 트래픽을 발생시킨 결과 Worm Detection System에서 탐지된 웜의 트래픽은 표 1과 같다. 그림 11은 이런 트래픽의 Destination IP주소의 분포도이다. 그림에서 볼 수 있듯이 첫 두 바이트 IP 주소는 전역에 랜덤 하게 분산되어있다.

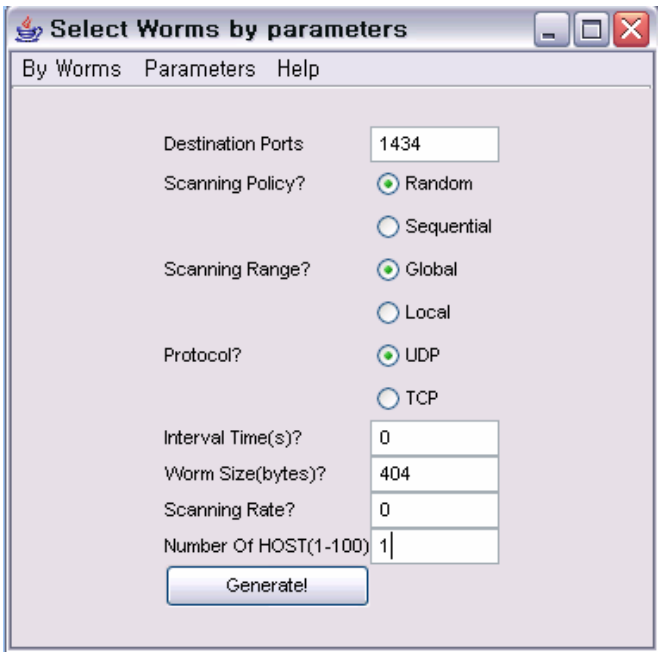

그림 10 Worm Traffic Generator의 입력화면

표 1 UDP 1434포트로 전체 IPv4 대역에 랜덤으로 스캐닝

Protocol	Port	Destination IP	Source IP	Source Port
17	1434	213.98.155.162	141.223.82.32	4700
17	1434	69.143.119.54	141.223.82.32	4718
17	1434	213.121.151.178	141.223.82.32	4730
17	1434	62.110.51.43	141.223.82.32	4739
17	1434	140.120.34.68	141.223.82.32	4767
17	1434	161.28.101.63	141.223.82.32	4772
17	1434	86.52.42.209	141.223.82.32	4897
17	1434	220.11.56.31	141.223.82.32	4910
17	1434	201.31.18.19	141.223.82.32	4922

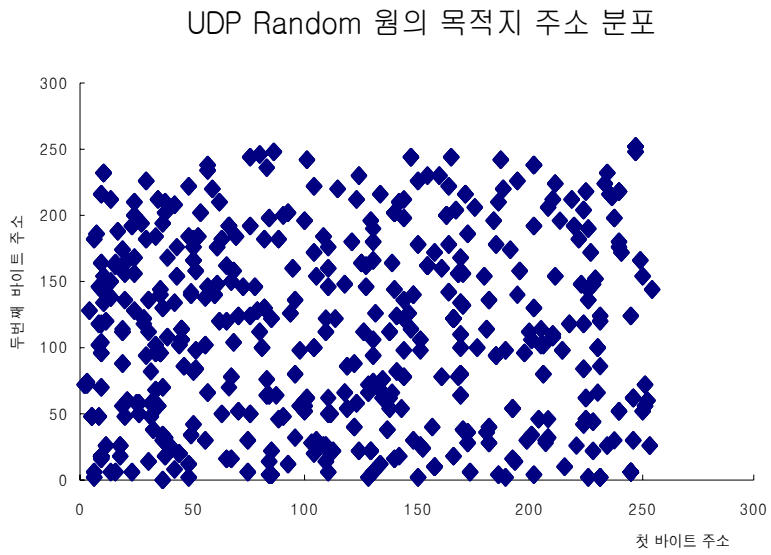

그림 11 Global-Random 웜의 첫 두 Octet의 분포도

4.5 Global-Sequential 웜의 탐지

TCP 445포트로 인터넷 전역으로 Sequential한 웜의 트래픽을 발생하여 Worm Detection System에서 탐지한 트래픽은 **표 2**와 같이 그 목적지주소가 순차적으로 올라감을 볼 수 있다. 인터넷 전역을 대상으로 하는 인터넷 웜의 트래픽은 랜덤으로 인터넷 전역 주소를 Seed로 찾은 후 그 이후의 주소에 Sequential하게 웜의 트래픽을 복사전파 하고 있다. 그림 12은 탐지한 인터넷 웜 트래픽의 목적지주소의 마지막 바이트가 sequential하게 증가하는 것을 보여준다.

표 2 TCP 445 포트 Global-Sequential 스캐닝 웜의 트래픽

Protocol	Port	Destination IP	Source IP	Source Port
6	445	68.92.23.55	141.223.82.32	14339
6	445	68.92.23.56	141.223.82.32	14595
6	445	68.92.23.57	141.223.82.32	14851
6	445	68.92.23.58	141.223.82.32	15107
6	445	68.92.23.59	141.223.82.32	15363
6	445	68.92.23.60	141.223.82.32	15619
6	445	68.92.23.61	141.223.82.32	15875
6	445	68.92.23.62	141.223.82.32	16131
6	445	68.92.23.63	141.223.82.32	16387

4.6 Local-Random/Sequential 웜의 탐지

일부 인터넷 웜은 로컬 스캐닝을 먼저 실행함으로써 감염속도를 향상

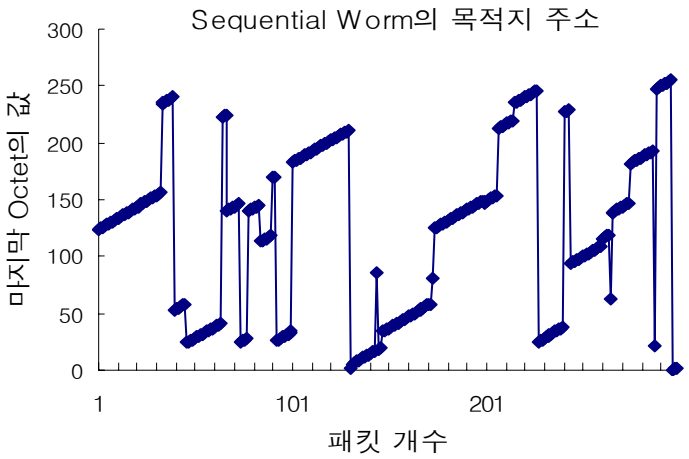

그림 12 인터넷 전역 주소로의 Sequential Scanning

시키고 있다. Blaster웜이 그 대표적인 예이다. Worm Traffic Generator로 로컬 네트워크를 목적지로 하는 Random/Sequential한 인터넷 웜 트래픽을 발생한 결과 Worm Detection System에서 탐지한 결과는 그림 13**오류! 참조 원본을 찾을 수 없습니다.**와 같다. 목적지주소의 3,4번째 바이트 주소의

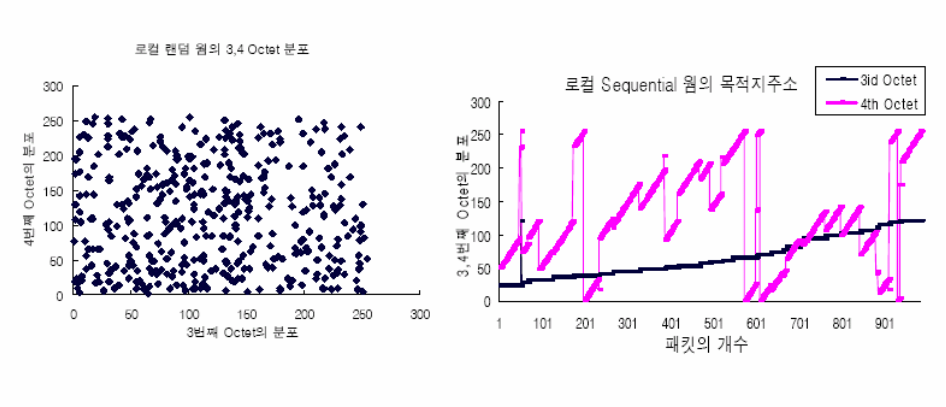

그림 13 로컬네트워크를 타겟으로 하는 Random/Sequential 웜

분포는 웜 트 래픽 발생 툴에서 발생한 것과 같이 랜덤 혹은 순차적으로 변하고 있다.

4.7 Worm Traffic Generator를 통한 검증의 결론

이 장에서는 먼저 실제 웜의 코드의 실행을 통하여 인터넷 웜 트래픽을 확보하였고 그 인터넷 웜의 트래픽을 Worm Detection System이 효과적으로 탐지함을 볼 수 있었다. 다음에 우리는 다양한 인터넷 웜의 트래픽을 발생하는 Worm Traffic Generator의 개발을 하였으며, 이런 툴을 사용하여 인터넷 웜의 탐지 알고리즘을 검증하는 과정을 설명하였다. 이런 과정을 통하여 TCP/UDP 웜, Global/Local 웜, Random/Sequential 웜 스캐닝 트래픽을 WDS가 False Positive없이 잘 탐지함을 볼 수 있었다. 다음 장에서 우리는 이런 시스템을 실시간으로 엔터프라이즈 네트워크에 적용했을 때 탐지결과를 분석한다.

5 POSTECH 네트워크에서 탐지결과

WDS가 정상적으로 인터넷 웜을 탐지하는지를 검증하기 위하여 우리는 실제 엔터프라이즈 네트워크에 3.3과 같이 알고리즘을 이용한 실시간 탐지 시스템을 구축하여 그 탐지 결과를 분석하였다.

탐지된 웜 트래픽의 특성을 분석함으로써 알고리즘에 의해 설계된 시스템이 정상적으로 인터넷 웜을 탐지하고 정상 트래픽을 분별해내는지를 알아보았다. 이 과정의 실험을 통하여 제안된 알고리즘이 엔터프라이즈 네트워크에서 인터넷 웜을 효과적으로 탐지할 수 있음을 검증하였다.

POSTECH 네트워크에서 수집되는 패킷 수는 1분에 300-500만개로 이런 패킷을 빠르게 처리하기 위하여 Hashing을 사용하였고 Database에 대한 조회를 최소한으로 줄이고 메인 메모리에서 대부분의 연산을 진행하였다. 모든 연산처리는 1분내에 완성 되여 그 결과가 Database에 저장된다. 시스템은 실시간으로 작동하고 웹 페이지를 통하여 실시간으로 결과를 확인할 수 있다.

5.1 탐지 결과의 분석

POSTECH네트워크에 구현된 탐지시스템은 2005년 12월 20일 01:58 과 21:00 에 각각 Random Scanning Worm, Sequential Worm을 발견하였다.

5.1.1 Sequential 스캐닝 웜

탐지시스템은 2005년 12월 20일 21:00에 Sequential 스캐닝 웜을 탐지하였다. 1분 동안에UDP 포트 5445로 1965개의 Sequential한 Destination IP주소로 스캐닝 하는 인터넷 웜에 감염된 호스트(141.223.52.51)를 탐지함을 그림 14로부터 볼 수 있다. 전형적인 sequential scanning 특징을 갖는 인터넷 웜 이다.

Time	Destinaiton Port	Infected Host	Protocol
2005.12.20 21:00	5445	141.223.52.51	UDP

No.	Dest Address	Bytes	Packets	SYN	ACK	Source Port
0	149.230.151.1	78	1	0	0	1027
1	149.230.151.2	78	1	0	0	1027
2	149.230.151.3	78	1	0	0	1027
3	149.230.151.4	78	1	0	0	1027
4	149.230.151.5	78	1	0	0	1027
5	149.230.151.6	78	1	0	0	1027
• • •						
1959	149.230.160.241	78	1	0	0	1027
1960	149.230.160.242	78	1	0	0	1027
1961	149.230.160.243	78	1	0	0	1027
1962	149.230.160.244	78	1	0	0	1027
1963	149.230.160.245	78	1	0	0	1027
1964	149.230.160.246	78	1	0	0	1027

그림 14 Sequential Worm의 탐지결과

5.1.2 Random 스캐닝 웜

Time	Destinaiton Port	Infected Host	Protocol
2005.12.20 01:58	64444	141.223.73.61	TCP

No.	Dest Address	Bytes	Packets	SYN	ACK	Source Port
0	217.250.255.107	82	6	0	0	1027
1	86.96.102.6	82	7	0	0	1027
2	58.11.84.91	82	8	0	0	1027
3	217.219.142.10	82	6	0	0	1027
4	84.167.219.62	82	6	0	0	1027
5	149.230.151.6	82	6	0	0	1027
• • •						
8708	60.237.174.120	82	8	0	0	1027
8709	85.97.137.132	82	1	0	0	1027
8710	60.212.162.17	82	4	0	0	1027
8711	217.245.192.111	82	5	0	0	1027
8712	219.95.156.133	82	4	0	0	1027
8713	84.5.0.224	82	3	0	0	1027

그림 15 Random 웜의 탐지결과

그림 15와 같이 가장 대표적인 Random Scanning 웜은 2005년 12월20일 01:58분에 탐지 되였다. 인터넷 웜에 감염된 141.223.73.61 IP 주소를 갖는 호스트는 랜덤 한 8714개의 IP 주소로 스캐닝 패킷을 발생하였다. 목적지 아이피 주소의 분포는 거의 전체 IPv4대역에 랜덤 하게 분포 되여 있다. 세 개의 Unallocated IP로 패킷을 전송한 것도 볼 수 있는데 정상적인 Application에서 우발적으로 보낼 수 있는 경우가 아님을 설명한다.

5.1.3 정상 트래픽

#of Suspicious Host	20	Analyzing Time <<2005.12.20 21:00>>
#of Sequential Worm	1	
#of Other Worm	0	

No.	Protocol	Dest Port	Packets	Syn Pakcets	#of Victims	#of Sequential	#of Worm
0	UDP	5445	1965	0	1	1	0
1	TCP	25	2205	2205	1	0	0
2	TCP	80	5668	5668	15	0	0
3	UDP	3309	3496	0	1	0	0
4	UDP	10025	1987	0	1	0	0
5	UDP	54171	1495	0	1	0	0

그림 16 2005년 5월13일 10:07분의 전체 탐지 결과

그림 16 은 2005년 12월 20일 :00분의 탐지 결과이다. 제일 윗부분에 핑크로 도색 된 행은 앞에서 설명한 Random Scanning Worm이고 나머지 포트들은 Suspicious List이다. 이중에서 우리가 알 수 있는 가장 대표적인 P2P Application인 E-Donkey가 사용하는 TCP 4662포트를 보면 1개의 Suspicious Host가 248개의 패킷을 1분에 Generate한 것을 알 수 있다. 그러나 인터넷 웜으로 판단되지 않은 것은 이 호스트는 Unallocated IP로 스캐닝을 하지 않기 때문이다. 다른 포트의 Suspicious Host들도 비슷하게 인터넷 웜에서 제외 되였다.

5.2 탐지 결과에 관한 결론

POSTECH 네트워크에서 구현된 탐지 시스템을 통하여 우리는

Random Scanning, Sequential Scanning웜, TCP/UDP웜에 대하여 효과적으로 탐지함을 볼 수 있었고 Suspicious List중에서 P2P 트래픽과 같은 정상 트래픽을 잘 분별함을 볼 수 있었다. 제안된 알고리즘은 엔터프라이즈 네트워크에서 효과적으로 인터넷 웜을 탐지할 수 있으며 이런 시스템은 실시간으로 인터넷 웜을 탐지하는 방안이 될 수 있다. 제안하는 인터넷 웜의 탐지 시스템의 확장은 인터넷 웜의 조기탐지의 해결책이기도 하다.

6 결론 및 향후 과제

우리는 엔터프라이즈 네트워크에 알맞은 인터넷 웜의 탐지 알고리즘에 대해서 제안하였고 그 알고리즘의 검증을 위하여 Snort시스템과의 비교분석을 하였으며 실제 POSTECH 네트워크에서의 구현을 통하여 탐지결과를 분석하였다. 검증을 하기 위하여 Worm Traffic Generator를 개발하였으며 이 툴은 향후 인터넷 웜의 연구에 도움을 줄 것이다.

인터넷 웜의 탐지 알고리즘에서 여러 가지 임계 값을 사용하였는데, 이런 임계 값의 변화가 인터넷 웜 탐지에 어떤 영향을 미치는지에 대한 연구는 향후 지속적으로 연구 되여야 할 과제이다.

다양한 네트워크 (C 클래스 네트워크 혹은 다른 Topology를 갖는 네트워크)에서 시스템을 적용하여 그 결과를 분석하는 실험은 알고리즘의 발전에 도움을 줄 것이다.

그리고 새로운 스캐닝방법(예를 들면 순차적 목적지 주소를 생성할 때 사이의 값이 1보다 큰 수인 순차적 스캐닝, 혹은 순열적 스캐닝)을 사용하는 인터넷 웜에 대한 대응에 관한 연구는 앞으로의 과제로 이어진다.

참 고 문 헌

[1] Charles Schmidt and Tom Darby, " The What, Why, and How of the 1988 Internet Worm,“ http://www.snowplow.org/tom/worm /worm.html, July 2001.

[2] David Moore, Colleen Shannon, Jeffery Brown, "Code-Red: A case study on the spread and victims of an Internet worm," Proc.2nd ACM Internet Measurement Workshop, ACM Press 2002, pp273-284, 2002.

[3] Moore, D, V.Paxson, S.Savage, C.Shannon, S.Staniford, N.Weaver, "Slammmer Worm Dissection: Inside the Slammer Worm," IEEE Security&Privacy, Vol.1 No.4 July-August 2003.

[4] F-Secure, “F-Secure Corporation Virus Glossary,” http://www.f-secure.com/virus-info/glossary.shtml.

[5] Symantec, http://securityresponse.symantec.com/avcenter /venc/data/w32.blaster.worm.html.

[6] CERT, "CERT Advisory CA-2001-26 Nimda Worm," http://www.cert.org/advisories/CA-2001-26.html.

[7] Symantec, http://securityresponse.symantec.com/avcenter/venc /data/w32.sasser.b.worm.html.

[8] Symantec, http://securityresponse.symantec.com/avcenter/venc /data/w32.witty.worm.html.

[9] F-Secure, http://www.f-secure.com/v-descs/scalper.shtml

[10] IANA, Internet Protocol V4 Address Space, http://www.iana.org/assignments/ipv4-address-space/.

[11] Bogon List, http://www.completewhois.com/bogons/.

[12] J. Wu, S. Vangala, L. Gao, and K. Kwiat, “An Efficient Architecture and Algorithm for Detecting Worms with Various Scan Techniques,” In Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS’04), February 2004.

[13] Ajay Gupta and Daniel C. DuVarney, “Using Predators to combat Worms and Viruses - a Simulation based study,” Proceedings in Annual Computer Security Applications Conference, ACSAC 2004

[14] Cliff C.Zou, Lixin Gao, Weibo Gong, Don Towsley, "Monitoring and Early Warning for Internet Worms," CCS’ 03, Oct 27-31, 2003.

[15] Vincent Berk, George. Bakos, “Designing a Framework for Active Worm Detection on Global Networks,” IWIA 2003, Darmstadt, Germany, March 2003, pp. 13-24.

[16] Shigang Chen and Yong Tang, "Slowing Down Internet Worms," 24th International Conference on Distributed Computing Systems

(ICDCS'04) Hachioji, Tokyo, Japan, March 24 - 26, 2004, pp. 312-319.
[17] Guofei Gu, Monirul Sharif, Xinzhou Qin, David Dagon,Wenke Lee and George Riley, “Worm Detection, Early Warning and Response Based on Local Victim Information”, Proceedings in Annual Computer Security Applications Conference, ACSAC 2004
[18] X. Qin, D. Dagon, G. Gu, and W. Lee, "Worm Detection Using Local network," Technical report, College of Computing, Georgia Tech., Feburary 2004.
[19] Bharath Madhusudan and John Lockwood, “Design of a System for Real-Time Worm Detection,” HOTI 12, Aug. 2004.
[20] George Bakos, Drs.Vincent H.Berk, "Early Detection of Internet Worm Activity by Metering ICMP Destination Unreachable Messages," 2003.
[21] Christian Kreibich, Jon Crowcroft,“Honeycomb-Creating Intrusion Detecton Signatures Using Honeyposts,” ACM SIGCOMM Computer Commnunications Forum Volumn 34, Number 1: January 2004
[22] Z. Chen, L. Gao, K. Kwiat, "Modeling the Spread of Active Worms," WORM 2003 on Network Sevurity, April, 2003
[23] Symantec Inc., http://www.symantec.com/.
[24] CAIDA, http://www.caida.org/.
[25] K.G.Anagnostakis, SSidiroglou, P.Akritidis,K.Xinidis,E.Markatos, A.D.Keromytis, “Detectiong Targeted Attacks Using Shadow Honeypots”, Pp. 129–144 of the Proceedings 14th USENIX Security Symposium
[26] T. Karagiannis, K. Papagiannaki, and M. Faloutsos,BLINC: Multilevel Traffic Classification in the Dark", ACM SIGCOMM, Philadelphia, PA, August 2005.
[27] Snort, http://www.snort.org
[28] Bro, http://bro-ids.org/
[29] Se-Hee Han, Myung-Sup Kim, Hong-Taek ju, and James W. Hong, “The Architecture of NG-MON: A Passive Network Monitoring System,” LNCS 2506, DSOM 2002, Montreal Canada, October 2002, pp. 16-27.

이 력 서

성 명: 조 룡권

생 년 월 일: 1971년 03월 19일

출 생 지: 중국 길림 성 도문 시

주 소: 중국 길림 성 연길 시 북산가

학 력

2000.09 – 2003.12: 중국 연변과학기술대학교 컴퓨터과학과기술 (B.S.)

2004.03 – 2006.02: 포항공과대학교 정보통신대학원 정보통신학과 (M.S.)

학 술 활 동

♦Conference Papers

Long-Quan Zhao, Seong-Chul Hong, Hong-Taek Ju and James Won-Ki Hong, "A Real-Time Network Traffic Based Worm Detection System for Enterprise Networks", Proc. of APNOMS 2005 Conference, Okinawa, Japan, Sep 27-30, 2005, pp.446-457.

Seong-Chul Hong, Long-Quan Zhao, Hong-Taek Ju and James W. Hong, “Worm Traffic Monitoring and Infected Hosts Detection Algorithm for Local Networks” IEEE IM 2005, Nice, France, May 2005.

조룡권, 주홍택, 홍원기, 주미리, 박응기, "SNMP 게이트웨이를 이용한 WBEM 기반의 통합관리 시스템", Proc. of KNOM 2005 Conference, Seoul, Korea, May 26-27, 2005, pp. 151-158.

♦Journal Papers

홍성철, **조룡권**, 주홍택, 홍원기, "엔터프라이즈 네트워크에서의 인터넷 웜 탐지를 위한 방법", KNOM Review, Vol. 7, No. 2, December 2004, pp. 11-20.

연구 활동

♦Projects

인터넷 웜 전파 및 활동에 따른 네트워크 트래픽 특성 연구, 국가보안연구소 Project, 2004

고속 네트워크에서 응용 트래픽 분류를 위한 네트워크 모니터링 방법 연구, KT Project, 2005

고속 네트워크에 적합한 트래픽 감시 및 제어 시스템 개발, 산자부 Project, 2003-2005